Decoherence free subspaces for two–access quantum channels

Maciej Demianowicz

Department of Atomic Physics and Luminescence, Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, ul. Narutowicza 11/12, PL80-233 Gdańsk, Poland & National Quantum Information Center in Gdańsk, ul. Wł. Andersa 27, PL81-824 Sopot, Poland & maciej@mif.pg.gda.pl

(Received 2008)

Abstract. In this paper we consider construction of decoherence free subspaces for two–access random unitary channels. First, we concentrate on hermitian unitary noise model U for a bi–unitary channel and show that in this case a code exists if the space of Schmidt matrices of an eigensubspace of U exhibits certain properties of decomposability. Then, we show that our technique is also applicable in a generic case and consider its application two tri- (quatro-, ...) unitary channels.

1. Introduction

Quantum information transmission [1, 2, 3, 4, 5] through a non trivial quantum channel inevitably involves occurrence of errors. These errors, handled in an incompetent way, may completely shadow an intended quantum message. In this context, methods of combating such errors naturally emerge as one of the main topics of the theory of quantum channels. Luckily, several useful techniques have been developed to overcome destructive influence of coupling to the environment (see, *e.g.*, [6, 7]). Among them, quantum error correction codes (QECC) are most widely recognized (see [8] and references therein). Methods of constructing QECC for quantum communication have been previously reported in the literature [9, 10, 11, 12]. However, all these proposals concerned bipartite communication. No general approach has been developed to treat the case of the larger number of users of a quantum network.

The present work is a step in an effort towards one such general approach. We concentrate on random unitary two–access channels and show how to construct decoherence free subspaces (DFS) for such channels. DFS are the carriers of quantum information on which it is completely safe from the influence of an environment, that is a quantum message goes undisturbed

through a channel (in the sense of a solely unitary operation). Since the recognition of their significance, DFS have drawn much attention (see, *e.g.*, [13] and references therein) and the concept found its experimental realizations [14, 15, 16]. In our case, we have to protect two signals from spatially separated independent senders, thus our DFS have to be factorizable according to this separation. It turns out that in the considered setting existence of DFS is exactly equivalent to the certain decomposability properties in the space of matrices of bounded rank. One of the motivations for the present paper was merging these concepts in a fruitful way.

The paper is organized as follows. In Section 2. we provide some background material. In Section 3. we state our main results. Next, we apply the results to the specific case of a qutrit–qutrit input. Then we discuss some generalizations.

2. Background

In this section we give some necessary background material. This includes quantum error correction conditions, spaces of matrices of bounded rank, and several miscellaneous mathematical facts. For the reader's convenience this part is quite voluminous.

2.1. Quantum channels

Quantum channel $\mathcal{L}$ is a completely positive trace–preserving map. Every channel admits the so–called Kraus (or Choi–Kraus, or operator–sum) representation as follows $\mathcal{L}(\varrho) = \sum_i A_i \varrho A_i^\dagger$ with $\sum_i A_i^\dagger A_i = \mathbb{1}$ [17, 18]. A random unitary channel is the one which has the representation $\mathcal{L}(\varrho) = \sum_i p_i U_i \varrho U_i^\dagger$, where U_i are unitary and $\sum_i p_i = 1$, $p_i \geq 0$. When such a channel has two Kraus operators, *i.e.*, $\mathcal{L}(\varrho) = pU_1\varrho {U_1}^\dagger + (1-p)U_2\varrho {U_2}^\dagger$, it is called bi–unitary. This kind of channels are the main interest of the present paper.

Channels can be classified upon the number of senders and receivers using them. We have the following types of channels according to such a classification [4, 19, 20, 21, 22]:

- bipartite — one sender and a single receiver,
- multiple access — several senders and one receiver,
- broadcast — one sender and several receivers,
- km–user — k senders and m receivers ($k, m > 1$).

In our reasonings we concentrate on two–access channels, that is multiple access channels with two senders.

Due to the possibility of a global rotation $U_1^\dagger \mathcal{L}(\varrho) U_1$ on the output of a channel, both in bipartite and multiple access case one can consider a simplified bi–unitary channel in general reasonings[1]

$$\mathcal{L}(\varrho) = p\varrho + (1-p)U\varrho U^\dagger. \tag{1}$$

For two–access channels it holds $\varrho = \varrho_1 \otimes \varrho_2$, where ϱ_i is an input of the i–th sender.

2.2. Quantum error correction

QECC is a subspace $\mathcal{C}$ of a larger Hilbert space $\mathcal{H}$. Equivalently, a code is defined to be the projection $P_\mathcal{C}$ onto $\mathcal{C} \subseteq \mathcal{H}$. One says that $\mathcal{C}$ is correctable if all states $\varrho = P_\mathcal{C} \varrho P_\mathcal{C}$ can be recovered after action of a channel using some decoding operation $\mathcal{D}$, that is $\mathcal{D} \circ \mathcal{L}(\varrho) = \varrho$. Such recovery operation exists if and only if $P_\mathcal{C} A_i^\dagger A_j P_\mathcal{C} = \alpha_{ij} P_\mathcal{C}$ for some hermitian matrix $[L]_{ij} = \alpha_{ij}$. These conditions are due to Knill and Laflamme (KL) [23].

When we have a larger number of senders we talk about local codes $\mathcal{C}_i$ prescribed for every sender. It is an immediate observation that KL conditions need only a little adjustment to serve for the case of MACs. Namely, we have (with the obvious notation):

OBSERVATION 1. *Local codes $\mathcal{C}_i$ are correctable for a MAC with Kraus operators $\{A_i\}$ with k inputs if and only if*

$$P_{\mathcal{C}_1} \otimes P_{\mathcal{C}_2} \otimes \ldots \otimes P_{\mathcal{C}_k} A_i^\dagger A_j P_{\mathcal{C}_1} \otimes P_{\mathcal{C}_2} \otimes \ldots \otimes P_{\mathcal{C}_k} = \alpha_{ij} P_{\mathcal{C}_1} \otimes P_{\mathcal{C}_2} \otimes \ldots \otimes P_{\mathcal{C}_k} \tag{2}$$

for some hermitian matrix $[L]_{ij} = \alpha_{ij}$.

This is true since the set of product codes is a subset of the set of all codes. In further parts, we use the denotation $R \otimes R'$ or $S \otimes S'$ for a code for a two–access channel and talk about $M \otimes N$ codes, where M, N denote dimensions of local codes.

In case of many usages of the channel, A_i are tensor products of Kraus operators in KL conditions. In this paper, however, we concentrate on a single usage of a channel. For one use of a bi–unitary channel, Eq. (1), KL conditions reduce to a *single* condition $PUP = \lambda P$ which for MACs takes the form [24]

$$R \otimes R' U R \otimes R' = \lambda R \otimes R'. \tag{3}$$

In some cases there is no need to perform recovery operation as the output of the channel is already the same as the input. In these cases, code spaces are

[1] Naturally, in a concrete case one needs to remember that $U = U_1{}^\dagger U_2$.

called *decoherence free subspaces* [13]. It is known that for bi–unitary channels DFS correspond to eigenspaces of degenerate eigenvalues of U [25]. Due to our interest in two–access channels we wish to find DFSs which factorize according to spatial separation of senders [2].

It is worth explicitly noting that our problem is exactly equivalent to finding a product subspace in a given subspace. One may think of this problem as of the generalization of the well known (solved) problem of existence of a product state in a given subspace [26, 27].

2.3. Spaces of matrices of bounded rank

A space of matrices of bounded (equal) rank is a space which contains only elements whose ranks are bounded by some prescribed number (or, besides the zero element, equal to it). The research on such spaces dates back to works by Flanders [28] and Westwick [29]. In quantum information theory the concept of spaces of matrices of bounded rank were recently used in Ref. [30]. If a space contains only elements of rank equal to k (besides zero element) we will be talking about k–spaces.

We will use $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ to denote space of matrices spanned respectively by $A_i, B_i, C_i, \ldots$. We define $r_m(\mathfrak{A}) \equiv \max_{M \in \mathfrak{A}} r(M)$. Further, we recall the concept of equivalence of spaces of matrices [28] and decomposability [29] We say that $\mathfrak{A}$ is *equivalent* to $\mathfrak{B}$ if there exist nonsingular matrices E,F such that $\mathfrak{A} = \{EBF,\ B \in \mathfrak{B}\}$. If these matrices are explicitly specified we talk about (E, F)*–equivalency*. A subspace $\mathfrak{A}$ of $a \times b$ matrices is called (t, s)*–decomposable* if it is equivalent to a subspace whose all elements have the form

$$A = \begin{pmatrix} [0]_{(a-t)\times(b-s)} & B_{(a-t)\times s} \\ C_{t\times(b-s)} & D_{t\times s} \end{pmatrix}, \quad A \in \mathfrak{A}. \tag{4}$$

When t, s are not specified, we will be just talking about a general fact of $(t + s)$*–decomposability*. Below we collect several important facts concerning decomposability in the spaces of 3×3 matrices of bounded rank. It holds true that [29, 31, 33]:

- three dimensional 2–subspaces are not 2–decomposable; moreover, up to an equivalence, there exists the unique such space — the space of skew–symmetric matrices [3],

[2]It is obvious that if we need no correction at the output, each of the local subspaces was send noiselessly. In this context, a question arises whether it would make any sense to introduce the notion of local decoherence free subspaces.

[3]It is an interesting coincidence: this space corresponds to the antisymmetric space of two qutrits via the identification states–matrices; antisymmetric spaces play an important role in many applications of quantum information theory.

- if $\mathfrak{B}$ is a 2–subspace then it necessarily holds that $\dim \mathfrak{B} \leq 3$,
- if a subspace $\mathfrak{B}$ with $r_m(\mathfrak{B}) = 2$ contains a rank one matrix then it is 2–decomposable,
- a subspace $\mathfrak{B}$ with $r_m(\mathfrak{B}) = 2$ and $4 \leq \dim \mathfrak{B} \leq 6$ is 2–decomposable (follows from above).

2.4. Space of states *vs.* space of Schmidt matrices

One of our main tools will be the well known one-to-one identification of pure states with matrices: with fixed orthonormal bases $|i\rangle$ and $|j\rangle$ for $\mathcal{H}_1 = \mathbb{C}^{d_1}$ and $\mathcal{H}_2 = \mathbb{C}^{d_2}$ respectively, one defines the *Schmidt matrix* of a state $|\psi\rangle = \sum_{ij} c_{ij}|ij\rangle$ to be $C = \sum_{ij} c_{ij}|i\rangle\langle j|$. For two states $|\phi\rangle$ and $|\psi\rangle$ with Schmidt matrices C and D it holds $\langle\phi|\psi\rangle = \mathrm{tr} C^\dagger D$. By direct calculation one finds that the transformation $|\psi\rangle \to U_1 \otimes U_2|\psi\rangle$ corresponds to $C \to U_1 C U_2^T$. Further, we define the *Schmidt rank* r of a state $|\psi\rangle$, denoted by $r(|\psi\rangle)$, to be the number of nonzero elements in its Schmidt decomposition and the *maximal Schmidt rank* r_m of the subspace $\mathcal{H}$ to be $r_m(\mathcal{H}) \equiv \max_{|\psi\rangle \in \mathcal{H}} r(|\psi\rangle)$. Obviously $r(|\psi\rangle) = r(C)$.

Let now $\mathcal{H} = \mathrm{span}\{|\gamma_i\rangle\}$ and $\mathfrak{H} = \mathrm{span}\{h_i\}$, where h_i is a Schmidt matrix of γ_i. Then $r_m(\mathcal{H}) = r_m(\mathfrak{H})$ due to the isomorphism between the space of unnormalized states and matrices. It is thus natural to transfer the idea of decomposability of the space of matrices to the space of states. Therefore we propose to use the following

PROPOSITION 2. *A subspace $\mathcal{H}$ is called (i,j)–decomposable if $\mathfrak{H}$ is so.*

3. Main results

In our reasonings we consider channels with d dimensional inputs (and thus d^2 dimensional output). We take U to be hermitian, which implies that it must have the form

$$U = P - Q, \tag{5}$$

where P and Q are both projections[1]. We further denote the eigensubspaces of U as $\mathcal{P} = P\mathcal{H}$ and $\mathcal{Q} = Q\mathcal{H}$ and let $\dim \mathcal{P} = p$ and $\dim \mathcal{Q} = q$.

We have the following[2] concerning the channel from Eq. (1) with U taken as in Eq. (5).

THEOREM 3. *A $M \otimes N$ DFS exists if and only if at least one of the subspaces $\mathcal{P}$ and $\mathcal{Q}$ is $(d-M, d-N)$–decomposable.*

[1] We naturally focus only on cases when U is not equal to $\mathbb{1}$.
[2] Note that a DFS for a *bipartite* channel with the considered noise model *always* exist.

PROOF. We put $\lambda = \pm 1$ in Eq. (3) as these are the suspicious values (see Section 2.2.). We have using Eq. (5):

$$R \otimes R'(P - Q)R \otimes R' = R \otimes R' \quad (\lambda = 1) \tag{6}$$

and

$$S \otimes S'(P - Q)R \otimes R' = -S \otimes S' \quad (\lambda = -1), \tag{7}$$

where R, S and R', S' are M and N dimensional projections respectively. It is evident that it is sufficient to conduct calculation for only one of the equations above as the sign of λ exchanges only the roles of P and Q. Therefore we concentrate on Eq. (6), which due to $P + Q = \mathbb{1}_d$ can be rewritten in two *equivalent* forms as

$$R \otimes R'QR \otimes R' = 0 \tag{8}$$

and

$$R \otimes R'PR \otimes R' = R \otimes R'. \tag{9}$$

Let us concentrate on the first equation (second equation will be further in some cases more convenient to draw conclusions about existence of codes). Assume

$$Q = \sum_{i=1}^{q} |\phi_i\rangle\langle\phi_i|, \quad |\phi_i\rangle = \sum_{kl} c_{kl}^{(i)} |kl\rangle, \quad k, l = 1, \cdots, d, \quad i = 1, \cdots, q \tag{10}$$

and let $[C_i]_{kl} = c_{kl}^{(i)}$. We can represent the projections as rotated projections written in the standard basis

$$R \otimes R' = U_1^\dagger \otimes U_2^\dagger \tilde{R} \otimes \tilde{R}' U_1 \otimes U_2, \quad \tilde{R} = \sum_{g=0}^{M-1} |g\rangle\langle g|, \quad \tilde{R}' = \sum_{h=0}^{N-1} |h\rangle\langle h|, \tag{11}$$

where U_1 and U_2 are unitary. Inserting Eqs (10) and (11) into Eq. (8) and taking into account that a matrix is zero iff all its elements are so we arrive at

$$\langle ij| \left(U_1 \otimes U_2 \left(\sum_m |\phi_m\rangle\langle\phi_m| \right) U_1^\dagger \otimes U_2^\dagger \right) |kl\rangle = 0,$$
$$i, k = 0, 1, \ldots, M-1 \quad j, l = 0, 1, \ldots, N-1. \tag{12}$$

In particular, this must be true for $ij = kl$, which gives

$$\textstyle\sum_m |\langle ij|U_1 \otimes U_2|\phi_m\rangle|^2 = 0,$$
$$i = 0, 1, \ldots, M-1; \quad j = 0, 1, \ldots, N-1 \tag{13}$$

and consequently for *all* values of m

$$\langle ij|U_1 \otimes U_2|\phi_m\rangle = 0,$$
$$i = 0, 1, \ldots, M-1; \quad j = 0, 1, \ldots, N-1. \tag{14}$$

This condition implies that off–diagonal terms vanish as well and thus Eq. (14) is *fully equivalent* to Eq. (8). Recalling the transformation rule for Schmidt matrices under local unitary rotations of a state (see Section 2.4.) condition above can be rewritten as

$$\langle i|U_1 C_m U_2^T|j\rangle = 0, \forall_m$$
$$i = 0, 1, \ldots, M-1; j = 0, 1, \ldots, N-1. \tag{15}$$

Denote $U \equiv U_1$ and $V \equiv U_2^T$. Eq. (15) states that all Schmidt matrices C_i must brought with the same unitary U, V to a form with the $M \times N$ zero matrix in the upper left corner. Notice that instead of full unitary matrices U, V we can consider their reductions, *i.e.*, isometries U_{isom} and V_{isom}, which are $M \times d$ and $d \times N$ respectively. Further, we need the following simple lemma

LEMMA 4. *Let A_i be complex $d \otimes d$ matrices and let V_1, V_2 be isometries. The condition $V_1 A_i V_2 = [0]_{M\times N}$ holds for all values of an index 'i' if and only if for all complex $\vec{\alpha} = (\alpha_1, \alpha_2, \cdots)$ it holds that $V_1(\sum_i \alpha_i C_i)V_2 = [0]_{M\times N}$.*

This means that the space $\mathfrak{C}$ must be (U, V)–equivalent to a space whose all elements have the zero $M \times N$ in the upper left corner. It suffices now to show that this equivalency means also $(d-M, d-N)$–decomposability, *i.e.*, to show that unitary matrices are as powerful as general full rank matrices in definition of decomposability (Eq. (4)). This what we are going to demonstrate now. Let X, Y be non singular matrices. If XC_iY has a $M \times N$ zero block it means that $X = ([\tilde{X}^T]_{d\times M}, [X']_{d\times(d-M)})^T$ and $Y = ([\tilde{Y}]_{d\times N}, [Y']_{d\times(d-N)})$ where $\tilde{X}$ and $\tilde{Y}$ are respectively rank M and N matrices such that $\tilde{X}C_i\tilde{Y} = [0]_{M\times N}$. It means that $\tilde{X}C_i$ has rank less than or equal to $d-N$ and the (possibly nonorthogonal) rows of $\tilde{Y}$ span the remaining N dimensions allowed in a d dimensional space. Thus it is enough to take isometry whose rows span the same space as the ones of $\tilde{Y}$ do to achieve zeroing of the resulting matrix. Arguing in the same way for left multiplication we arrive at conclusion that both $\tilde{X}$ and $\tilde{Y}$ can be replaced by isometries which can be completed to unitaries. This ends the proof of the theorem. ■

Let now $\mathfrak{D}$ be the space spanned by Schmidt matrices of the projection P. We can immediately conclude the following simple necessary condition for the existence of a DFS

COROLLARY 5. *If there is a $M \otimes N$ DFC then either of the following holds*

$$r_m(\mathfrak{C}) \leq 2d - (M+N), \tag{16}$$

$$r_m(\mathfrak{D}) \leq 2d - (M+N). \tag{17}$$

Alternatively

$$r_m(\mathcal{Q}) \leq 2d - (M+N), \tag{18}$$

$$r_m(\mathcal{P}) \leq 2d - (M+N). \tag{19}$$

PROOF. Follows from Theorem 3. and the property $r(B) \leq t + u - r(A) - r(C) + r(ABC)$ valid for arbitrary matrices $A_{s\times t}$, $B_{t\times u}$, $C_{u\times v}$. The latter can be proved by using twice the Sylvester's inequality [34].■

For further practical purposes, it is convenient to rewrite Theorem 3. as follows

COROLLARY 6. *A $M \otimes N$ DFS exists if and only if either of the following holds:*
i) there exist isometry $[V_1^Q]_{M\times d}$ such that

$$r\left(\mathcal{C}_V^Q := \begin{pmatrix} V_1^Q C_1 \\ V_1^Q C_2 \\ \cdots \\ V_1^Q C_q \end{pmatrix}\right) \leq d - N, \tag{20}$$

ii) there exists isometry $[V_1^P]_{M\times d}$ such that

$$r\left(\mathcal{C}_V^P := \begin{pmatrix} V_1^P D_1 \\ V_1^P D_2 \\ \cdots \\ V_1^P D_p \end{pmatrix}\right) \leq d - N. \tag{21}$$

We observe that we can give immediately a rough bound on dimensions of an input for which a $M \otimes N$ code surely exists for a fixed q.

COROLLARY 7. *If i) $q = 2$ and $d \geq M+N$ or ii) $q > 3$ and $d \geq \min\{Mq+N, Nq+M\}$ then there always exists a $M \otimes N$ DFS for the considered channel.*

PROOF. The first part follows from the generalized Schur decomposition theorem [35] stating that for any two complex matrices A, B there exist unitary transformations U, V such that UAV and UBV are both upper or lower triangular at the same time.

As to the second part. M rows of q Schmidt matrices of Q span at most Mq dimensional subspace. Since $d \geq Mq + N$ there is still enough

space for N orthogonal vectors in the whole d dimensional space. Taking $U_{isom} = (\mathbb{1}_{M\times(d-M)} \quad [0]_{M\times M})$ and V_{isom} to consist of the mentioned N vectors as matrix columns we produce $M \times N$ zero matrix. Analogous reasoning applies to right multiplication by V_{isom} and choosing U_{isom} to consist of proper columns.■
Naturally, the same holds for p in place of q.

4. Applications: qutrit-qutrit input case

We now move to the specific case of a qutrit inputs to the channel. Our main interest will be in the construction of $2\otimes 2$ codes. The cases $1\otimes 2$ $(2\otimes 1)$ are not interesting for us as such codes correspond to a non–zero rate only on the single wire of the network, on the other hand codes $2\otimes 3$ $(3\otimes 2)$ correspond to the situations when one of the parties can send with maximum rate, which clearly requires very specific type of noise (although not of the form $U'\otimes \mathbb{1}$ or $\mathbb{1}\otimes U'$ as one can check).

Direct application of Theorem 3. relying on finding proper isometries U_{isom} and V_{isom} giving zero blocks in the corner of all the matrices is a tedious task when $3 \leq q \leq 7$. In these cases, one is thus recommended to consult Refs. [29, 31, 33] for elegant techniques. Some relevant results have been given in Section 2.3.

In what follows we concentrate on the $q = 2$ case. In Ref. [31], it has been shown that every two dimensional spaces of matrices with $r_m \leq k$ is k–decomposable. However, no explicit distinction between different kinds of decomposability has been given. We thus feel inclined to provide detailed discussion concerning $(1,1)$–decomposability in the relevant case of $d = 3$. The result is summarized in the following theorem.

THEOREM 8. *If $q = 2$ then a $2\otimes 2$ code exists if and only if $r_m(\mathfrak{C}) \leq 2$ <u>and</u> $\mathfrak{C}$ is <u>not</u> a $(0,2)$ or $(2,0)$–decomposable 2–subspace.*

PROOF. (The proof is constructive) It is obvious from the upcoming Lemma 4. that we need only to solve Eq. (6), that is to take $\lambda = +1$. Thus, no considerations concerning decomposability of $\mathfrak{D}$ are required. Further, it is also evident from Corollary 3. that it must be that $r_m(\mathfrak{C}) \leq 2$ implying that $r(C_i) \leq 2$. We assume that we have already passed to the (W_1, W_2)–equivalent space where W_1 and W_2 come from the singular value decomposition of C_2. In such basis we assume these matrices to be

$$C_1 = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & a \end{pmatrix}, \quad a + b > 0. \tag{22}$$

It is further assumed that $r(C_1) \leq r(C_2)$.

Suppose $r_m(\mathfrak{C}) = 1$. It is a simple observation that in this case, in the matrix C_1 only the last row or column (not at the same time obviously) is non zero. Existence of a code is thus a trivial fact.

Suppose now that $\mathfrak{C}$ contains an element of rank 2. W.l.o.g. we can assume that C_2 is such an element, that is both a and b are greater than zero. Condition $r_m(\mathfrak{C}) \leq 2$ is fulfilled if for all β it holds that $\det(C_1 + \beta C_2) = 0$, which happens when [1]

$$c_{11} = 0, \quad \det C_1 = 0, \quad a c_{12} c_{21} + b c_{13} c_{31} = 0, \tag{23}$$

which we hereafter assume to hold. We now further consider specific cases. Suppose $(c_{12}, c_{13}) \neq (0,0)$ and $(c_{21}, c_{31}) \neq (0,0)$. Take

$$V_1^Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{a c_{12}}{N_1} & \frac{b c_{13}}{N_1} \end{pmatrix}, \quad V_2^Q = \begin{pmatrix} 1 & 0 \\ 0 & \frac{a c_{21}}{N_2} \\ 0 & \frac{b c_{31}}{N_2} \end{pmatrix}, \tag{24}$$

with normalization constants $N_1 = \sqrt{a^2|c_{12}|^2 + b^2|c_{13}|^2}$ and $N_2 = \sqrt{a^2|c_{21}|^2 + b^2|c_{31}|^2}$. With this choice of isometries, using last condition of Eq. (23), one can verify that it holds for the matrix elements that $[V_1^Q C_1 V_2^Q]_{11} = [V_1^Q C_1 V_2^Q]_{12} = [V_1^Q C_1 V_2^Q]_{21} = 0$ and $V_1^Q C_2 V_2^Q = [0]_{2\times 2}$; using last two conditions of Eq. (23) one arrives at $[V_1^Q C_1 V_2^Q]_{22} = 0$. This proves existence of a code.

If $(c_{12}, c_{13}) \equiv (0,0)$ and $(c_{21}, c_{31}) \equiv (0,0)$ by previously mentioned generalized Schur decomposition and a simple swapping of rows we can transform both matrices simultaneously according to

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & \star & \star \\ 0 & \star & \star \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & 0 \\ 0 & \star & \star \\ 0 & 0 & \star \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \star \\ 0 & \star & \star \end{pmatrix} \tag{25}$$

which outputs the proper code.

Suppose $(c_{12}, c_{13}) \equiv (0,0)$ and $(c_{21}, c_{31}) \neq (0,0)$. Setting $[V_1^Q]_{ij} = v_{ij}$ We have

$$\mathcal{C}_V^Q = \begin{pmatrix} v_{12}c_{21} + v_{13}c_{31} & v_{12}c_{22} + v_{13}c_{32} & v_{12}c_{23} + v_{13}c_{33} \\ v_{22}c_{21} + v_{23}c_{31} & v_{22}c_{22} + v_{23}c_{32} & v_{22}c_{23} + v_{13}c_{33} \\ 0 & b v_{12} & a v_{13} \\ 0 & b v_{22} & a v_{23} \end{pmatrix}, \tag{26}$$

[1] Conditions of this type are standard in analyses of spaces matrices of bounded rank.

which must be rank one (all rows, equivalently columns, must be proportional to each other). There are two (in principle non exclusive) possibilities for this to hold: (i) $bv_{12} = av_{13} = 0$ and $bv_{22} = av_{23} = 0$ or (ii) $v_{12}c_{21} + v_{13}c_{31} = 0$ and $v_{22}c_{21} + v_{23}c_{31} = 0$. The first alternative cannot be true in any case since $a > 0$, $b > 0$ and this would entail the fact that $v_{12} = v_{13} = v_{22} = v_{23} = 0$ which is impossible because of the isometric character of V_1^Q. We thus have $v_{12}c_{21} + v_{13}c_{31} = 0$ and $v_{22}c_{21} + v_{23}c_{31} = 0$. W.l.o.g. we can set $v_{22} = v_{23} = 0$ reducing the problem to finding conditions under which there exists such γ that the system of equations

$$\begin{aligned} v_{12}c_{21} + v_{13}c_{31} &= 0, \\ \gamma b v_{12} &= v_{12}c_{22} + v_{13}c_{32}, \\ \gamma a v_{13} &= v_{12}c_{23} + v_{13}c_{33}, \end{aligned} \tag{27}$$

has a nontrivial solution, where the last two equations are the requirement that the first row is proportional to the third one. This is possible if there exists such γ that

$$r\left(\begin{pmatrix} c_{21} & c_{22} - \gamma a & c_{23} \\ c_{31} & c_{32} & c_{33} - \gamma b \end{pmatrix}\right) \leq 1. \tag{28}$$

Recalling that the first row of C_1 is now equal to zero, it can be equivalently written as $r(C_1 - \gamma C_2) \leq 1$, which is simply the obligation for the subspace $\mathcal{Q}$ to contain a rank one element (there must *exist* such γ, not for all of them it must hold) or, in other words, *not* to be a 2–subspace. The case of $(c_{12}, c_{13}) \neq (0,0)$ and $(c_{21}, c_{31}) = (0,0)$ can be treated obviously in a similar manner and we get that there must exist such γ that

$$r\left(\begin{pmatrix} c_{12} & c_{13} \\ c_{22} - \gamma b & c_{23} \\ c_{32} & c_{33} - \gamma b \end{pmatrix}\right) \leq 1 \tag{29}$$

with the same conclusion. This exhausts all possibilities. ■

With no effort we can extend our result to the case $q = 7$. Namely, we have

THEOREM 9. *If $q = 7$ then a $2 \otimes 2$ code exists if and only if $r_m(\mathfrak{D}) \leq 2$ <u>and</u> $\mathfrak{D}$ is <u>not</u> a $(0,2)$ or $(2,0)$–decomposable 2–subspace.*

Notice that at no point in the proof have we made an assumption about orthogonality of the matrices.

We conclude this section with some observations.

FACT 10. *Let P, Q, R be projectors with $r(P) = p$, $r(Q) = q$, $r(R) = pq$. The following holds $P \otimes QRP \otimes Q = P \otimes Q$ if and only if $R = P \otimes Q$.*

This means that in some situations we can approach the problem of deciding existence of a code more directly for $q = 4, 5$. Specifically, for $q = 4$ we check whether Q is product $2 \otimes 2$. Positive answer resolves the matter on the spot. If the answer is negative, we need to check $\mathfrak{D}$ for the decomposability . By analogy, if $q = 5$ we check whether P is $2 \otimes 2$ product, if it is we immediately have a code, if not — we test $\mathfrak{C}$ for decomposability. Using this method we can easily show that $\lambda = -1$ and $\lambda = +1$ cannot belong to $\Lambda_{2\otimes 2}$ at the same time. We call this impossibility the *uniqueness* of DFS. We state this fact as follows:

OBSERVATION 11. *$2 \otimes 2$ DFS for the considered noise model in case of $d = 3$ is unique.*

Interestingly, the uniqueness is more powerful as the following holds true:

OBSERVATION 12. *If there is a $2 \otimes 2$ DFS for $d = 3$ there exists no code corresponding to other values of λ.*

The proof of this fact is given in [37].

It should be noted that for the noise model introduced in the beginning, standard (non–product) DFS always exist, which follows from high degeneracy of spectrum.

4.1. Examples

Here we provide several illustrations to the results obtained above. We assume Eq. (10) to hold in what follows; in every case our concern is the existence of a $2 \otimes 2$ code. We itemize our examples below.

- $q = 1$

$$|\phi_1\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle) \tag{30}$$

  A code does not exist since the necessary condition (Corollary 3.) is not fulfilled as $r(C) = 3$.

- $q = 2$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |22\rangle)$$
$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |21\rangle)$$

  $\mathfrak{C}$ is a $(0, 2)$–decomposable 2–subspace and as such it is not $(1, 1)$–decomposable thus a code does not exist (see Theorem 4.).

- $q = 2$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|02\rangle + |10\rangle)$$
$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |20\rangle)$$

$\mathfrak{C}$ is a 2–subspace but its $(1,1)$–decomposability can be easily seen. A code exists and is given by $P_C = R \otimes R' = P_{12} \otimes P_{12}$, where $P_{12} = |1\rangle\langle 1| + |2\rangle\langle 2|$.

- $q = 3$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$
$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|12\rangle - |21\rangle)$$
$$|\phi_3\rangle = \frac{1}{\sqrt{2}}(|02\rangle - |20\rangle)$$

Q is a projection onto the antisymmetric subspace. A DFS does not exist. This projection corresponds to the noise with $U = SWAP$. In fact, there is also no other code for two–access transmission through such a channel (see [37]).

- $q = 4$

$$|\phi_1\rangle = |00\rangle$$
$$|\phi_2\rangle = |01\rangle$$
$$|\phi_3\rangle = |10\rangle$$
$$|\phi_4\rangle = |11\rangle$$

Q is product itself so a code definitely exists. Alternatively we could check $\mathfrak{C}$ and $\mathfrak{D}$ which will result in $(1,1)$–decomposability of $\mathfrak{D}$.

- $q = 4$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\phi_2\rangle = |20\rangle$$
$$|\phi_3\rangle = |21\rangle$$
$$|\phi_4\rangle = |22\rangle$$

It holds that $r_m(\mathcal{Q}) = 3$ so $\mathcal{Q}$ cannot be $(1,1)$–decomposable. On the other hand Q itself is not product so there is no code at all. It is

interesting that $\mathcal{Q}$ contains a rank three vector $1/\sqrt{3}(|00\rangle + |11\rangle + |22\rangle)$ but its complement contains vectors of rank at most two [38]. The latter leads to

OBSERVATION 13. *In a* $3 \otimes 3$ *Hilbert space, the complement* $\mathcal{P}$ *of the four dimensional subspace* $\mathcal{Q}$ *with* $r_m(\mathcal{Q}) = 3$ *may have* $r_m(\mathcal{P}) = 2$.

5. Generalization

In this section we show that our reasoning can be applied to a more general type of noise. In fact, it turns out that a generic case in which a bipartite decoherence free subspace exists, which serves as a starting point of our discussions, can be treated by our technique. W.l.o.g. we focus on $2 \otimes 2$ codes in the $d = 3$ case.

As we have already mentioned, a bipartite DFS exists only if the spectrum of U is sufficiently degenerate, in present case it must be at least four–fold degeneracy. This observation immediately leads to the conclusion that we can successfully consider the following noise model

$$U = P_0 + \sum_{k \neq 0} \mathrm{e}^{\mathrm{i}\delta_k} P_k \tag{31}$$

with at least rank four projection P_0 and arbitrary phases δ_i. If at least three of them are distinct, it follows from the theory of higher rank numerical range that only $\lambda = +1$ needs to be considered. If $\delta_i = \pi$ for $i = 1, 2, 3, 4$ then both $\lambda = -1$ and $\lambda = +1$ have to be taken into account. Note that a phase in front of P_0 is redundant as it corresponds to a global phase which cancels when $U(\cdot)U^\dagger$ is applied (this phase irrelevance also applies to the noise we considered so far).

To support our claim concerning validity of the previous analyses, we provide a quick calculation . Let us assume that only $\lambda = +1$ is possible. Since $\sum_i P_i = \mathbb{1}$, we can replace U with $U = \mathbb{1} + \sum_{k \neq 0} (\mathrm{e}^{\mathrm{i}\delta_k} - 1) P_k$. Inserting this into the KL condition with $\lambda = 1$ we obtain

$$R \otimes R' (\mathbb{1} + \sum_{k \neq k_0} (\mathrm{e}^{\mathrm{i}\delta_k} - 1) P_k) R \otimes R' = R \otimes R' \tag{32}$$

which further gives

$$R \otimes R' (\sum_{k \neq 0} (\mathrm{e}^{\mathrm{i}\delta_k} - 1) P_k) R \otimes R' = 0. \tag{33}$$

Assume now that for each k we have $P_k = \sum_m |\gamma_k^m\rangle\langle\gamma_k^m|$, then for all i, j, α, β it must hold that

$$\sum_k (\mathrm{e}^{\mathrm{i}\delta_k} - 1) \langle ij| U_1 \otimes U_2 \sum_m |\gamma_k^m\rangle\langle\gamma_k^m| U_1^\dagger \otimes U_2^\dagger |\alpha\beta\rangle = 0. \tag{34}$$

Considering diagonal terms *i.e.*, $ij = \alpha\beta$ leads to

$$\sum_k (\mathrm{e}^{\mathrm{i}\delta_k} - 1) \sum_m |\langle ij|U_1 \otimes U_2|\gamma_k^m\rangle|^2 = 0. \tag{35}$$

Since $\mathrm{Re}(\mathrm{e}^{\mathrm{i}\delta_k} - 1) < 0$ (phase equal to zero has been previously eliminated) we conclude that

$$\forall_{k,m}\forall_{i,j} \;\; \langle ij|U_1 \otimes U_2|\gamma_k^m\rangle = 0, \tag{36}$$

which, if we denote by C_k^m Schmidt matrices of γ_k^m, as previously is equivalent to

$$\forall_{k,m}\forall_{i,j} \;\; \langle i|U_1 C_k^m U_2^T|j\rangle = 0. \tag{37}$$

This means that the preceding analysis is valid for any U with at least four–fold degeneracy of the spectrum.

We can take a step further in our generalizations and consider the triunitary channel

$$\Lambda(\varrho_1 \otimes \varrho_2) = (1-p-q)\varrho_1 \otimes \varrho_2 + pU(\varrho_1 \otimes \varrho_2)U^\dagger + qV(\varrho_1 \otimes \varrho_2)V^\dagger \tag{38}$$

with

$$U = P_0 + \sum_k \mathrm{e}^{\mathrm{i}\alpha_k} Q_k, \quad V = P_0 + \sum_k \mathrm{e}^{\mathrm{i}\beta_k} Q_k$$

with $r(P_0) \geq 4$, $\alpha_i \neq \beta_i$ and arbitrary Q_k (orthogonal to P_0). This stems from the fact that in this case we need to solve system of equations stemming from KL conditions

$$R \otimes R' U R \otimes R' = \lambda_1 R \otimes R' \tag{39}$$

$$R \otimes R' V R \otimes R' = \lambda_2 R \otimes R' \tag{40}$$

$$R \otimes R' U^\dagger V R \otimes R' = \lambda_3 R \otimes R'. \tag{41}$$

Taking $\lambda_i = +1$ we arrive at the same type of equations as previously. Due to the specific form of the unitaries, it is sufficient to consider only one of the equations and for the rest conclusion is drawn automatically. Increment in number of unitaries is naturally possible.

6. Conclusions

Summarizing, we have considered construction of decoherence free subspaces for biunitary two–access channels. Starting with a hermitian noise model we showed that the problem is directly related to the characterization of spaces of matrices of bounded rank, an area of linear algebra, which is

quite well established and understood. We further generalized the approach to arbitrary noise models and triunitary channels. To the best of our knowledge this the first time when analyses of spaces of matrices of bounded rank enter the field of quantum error correction.

It is not clear to what extent the techniques we used can be applied to channels with arbitrary Kraus operators. Notice, however, that using our technique we can solve Eq. (3) for any operator with a spectrum with fixed real or imaginary part.

We encourage the reader to consult Ref. [37] for methods of constructing higher entropy codes.

Acknowledgments

Discussions with P. Horodecki and K. Życzkowski are gratefully acknowledged. The author is supported by Gdańsk University of Technology through the grant "Dotacja na kształcenie młodych kadr w roku 2011".

Bibliography

1. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
2. S. Lloyd, Phys. Rev. A. **55**, 1613 (1997).
3. H. Barnum, M.A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).
4. H. Barnum, E. Knill, and M.A. Nielsen, IEEE Trans. Inf. Th. **46**, 19 (2000).
5. I. Devetak, IEEE Trans. Inf. Th. **IT-55**, 44 (2005).
6. M. S. Byrd, L.-A. Wu, and D. A. Lidar, J. Mod. Opt. **51**, 2449 (2004).
7. D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, Quant. Inf. Comp. **6**, 383 (2006).
8. F. Gaitan, *Quantum Error Correction and Fault Tolerant Quantum Computing* (CRC Press, 2008).
9. A. Steane, Rep. Prog. Phys. **61**, 117 (1998).
10. A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996).
11. D. Gottesman, Phys. Rev. A 54, 1862 (1996); D. Gottesman, Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997), eprint quant-ph/9705052.
12. M.–D. Choi, D. W. Kribs, and K. Życzkowski, Rep. Math. Phys. **58**, 77 (2006).
13. D. A. Lidar and K. B. Whaley, Decoherence-free subspaces and subsystems, in Irreversible Quantum Dynamics, F. Benatti and R. Floreanini, Eds., vol. **622** of Lecture Notes in Physics, pp. 83120, Springer, Berlin, Germany, 2003.
14. P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, Science **290**, 498 (2000).
15. T. Yamamoto, K. Hayashi, S. K. Ö zdemir, M. Koashi, and N. Imoto, Nature Photonics **2**, 488 (2008).

16. D. A. Pushin, M. G. Huber, M. Arif, and D. G. Cory, Phys. Rev. Lett. **107**, 150401 (2011).

17. M.–D. Choi, Lin. Alg. Appl. **10**, 285 (1975).

18. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer - Verlag, Berlin, 1983).

19. M. Demianowicz and P. Horodecki, Phys. Rev. A **74**, 042336 (2006).

20. J. Yard, I. Devetak, and P. Hayden, IEEE Trans. Inf. Th. **54** 3091 (2008).

21. M. Demianowicz and P. Horodecki, Phys. Lett. A **374**, 2914 (2010).

22. J. Yard, P. Hayden, and I. Devetak, IEEE Trans. Inf. Th. **57**, 7147 (2011).

23. E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

24. Motivated by the form of KL conditions, the authors of [12] introduced the notion of higher rank numerical range as the tool helpful in finding QECs for bipartite channels. For an arbitrary operator A, higher rank (or rank–k) numerical range is the set $\Lambda_k(A) = \{\lambda \in \mathbb{C} : PAP = \lambda P \quad \text{for some} \quad P \in \mathcal{P}_k\}$, where $\mathcal{P}_k$ is the set of all rank k projections. This notion and the form of KL conditions for MACs prompted us to introduce the notion of $k_1 \otimes k_2 \otimes \cdots$ *product higher rank numerical range*, which for an operator A is defined to be $\Lambda_{k_1\otimes k_2\otimes\cdots}(A) = \{\lambda \in \mathbb{C} : R\otimes R'\otimes\cdots AR\otimes R'\otimes\cdots = \lambda R\otimes R'\otimes\cdots \quad \text{for some} \quad R \in \mathcal{P}_{k_1},\ R' \in \mathcal{P}_{k_2},\ldots\}$. Properties of this set will be considered in [37].

25. D. W. Kribs, A. Pasieka, and K. Życzkowski, Open Syst. Inf. Dyn. **15**, 329 (2008).

26. K. R. Parthasarathy, Proc. Indian Acad. Sci. (Math. Sci.) **114**, 365 (2004).

27. Z. Puchała, P. Gawron, J. A.Miszczak, Ł. Skowronek, M.–D. Choi, and K. Życzkowski, Linear Algebra Appl. **434**, 327 (2011); P. Gawron, Z. Puchała, J. A.Miszczak, Ł. Skowronek, and K. Życzkowski, J. Math. Phys. **51**, 102204 (2010).

28. H. Flanders, London Math. Soc. **37**, 10 (1962).

29. R, Westwick, Lin. Alg. Appl. **5**, 49 (1972).

30. T. S. Cubitt, A. Montanaro, and A. Winter, J. Math. Phys. **49** 022107 (2008).

31. M. D. Atkinson and N. M. Stephens, Quart. J. Math. Oxford Ser. **28**, 205 (1978).

32. M. D. Atkinson and S. Lloyd, Quart. J. Math. Oxford Ser. **31**, 253 (1980).

33. M. D. Atkinson and S. Lloyd, J. Austral. Math. Soc. (Series A) **30**, 473 (1981).

34. H. Lütkepohl, *Handbook of Matrices* (John Wiley and Sons, Chichester, 1996).

35. G. W. Stewart, SIAM J. Numer. Anal. **9**, 669 (1972).

36. It is clear from the content of [24] that we will be trying to decide whether $+1 \in \Lambda_{M\otimes N}$ or $-1 \in \Lambda_{M\otimes N}$ and in case it does we will looking for the projections corresponding to this value. In [37] we will also consider other cases.

37. M. Demianowicz, P. Horodecki, and K. Życzkowski, *Multiaccess quantum communication and product higher rank numerical range*, arXiv:1209.0119.

38. The example has been suggested to the author by P. Horodecki.